秘密

お客様に対する基本行動

[ISK 社員行動基準]

（1） 常にお客様の視点に立ち、全てのプロセスにおいて安全性に十分配慮し、かつ高品質なサービスを提供しなければならない。

（2） 提供するサービスは、お客様の企業価値向上に貢献するとともに、社会の発展に資するものでなければならない。

（3） お客さまの生産性向上に貢献し続けるために、常に新たな価値の創造に努めなければならない。

（4） お客様およびお取引先等との契約を厳守し、信頼を保たなければならない。

機密情報管理・個人情報保護の徹底

アイ・エス・ケー株式会社　内部統制部門
コンプライアンス委員会
リスクマネジメント委員会

「お客様対応作業における遵守事項」

用語の定義

本遵守事項における用語の定義は以下の通り。

「お客様情報」とは、お客様の保有する情報（お客様の個人情報を含む）を指し、「預かる」、「提供される」、「開示される」場合のほか、「業務遂行過程で知り得た」ものも含みます。

「お客様対応作業」とは、「お客様の構内で行われる作業」、「お客様のシステム・ネットワークへの接続・修正等の作業」、「お客様情報をお預かりして処理する作業」のいずれかを指します。

「業務責任者」とは、お客様から委託を受けたお客様対応作業に関する会社の管理者を指します。

「電子機器」とは、PC、携帯情報端末、携帯電話、記録装置等を指します。

「記録媒体」とは、USB メモリ、FD、CD、DVD、ポータブル HDD、MO、メモリカード（例：SD カード）等を指します。

はじめに

（1） 本「お客様対応作業における遵守事項」（以下本遵守事項という）に記載されている事項を遵守し、常にお客様のシステム、ネットワークおよびお客様情報、個人情報等に係る安全確保を十分に行う。

（2） お客様対応作業を開始する場合には、まず、自らが遵守すべきことを認識する。

（3） 本遵守事項は、最低限遵守すべき事項をまとめたものであり、お客様が本遵守事項の各項目に関し、より厳しい基準を設けている場合はそれに従う。

（4） 「お客様の指示、承諾」をお客様または会社の指定により「具体的な監督者またはそれに準ずる責任者の指示、承諾」と定めている場合は、それに従う。

（5） 現在の業務において、該当しない遵守項目についてもセキュリティ対策の重要性を認識し、内容を理解する。

（6） 「お客様対応作業における遵守事項」に加え、関連法規、会社の指示事項、お客様所定の構内作業時ルール等（以下、総称してルール等という）も併せて遵守する。

（7） 業務責任者は、本遵守事項、（6）に定めるルール等を管理下の従事者に確実に遵守させるために、必要かつ適切な監督（遵守状況の定期的確認、注意喚起、逸脱行為または不遵守の発見および是正等）を実施する。

1． お客様情報の取扱い原則

1-1（お客様情報の開示）

お客様情報を、当該お客様対応作業遂行中のみならず、遂行後もお客様の書面による事前の承諾を得ることなく会社以外の個人法人および団体に開示し、または漏えいしない。

また、相手が会社の役員、従業員（契約社員、派遣社員を含む）であっても、当該お客様対応作業の遂行に関係のない者にお客様情報を開示し、または漏えいしない。

1-2（契約等の遵守）

お客様情報はお客様との取り決め（契約、覚書　等）の目的のみにおいて使用する。

1-3（お客様情報の複製）

お客様情報を、会社の書面による事前の承諾を得ることなく当該お客様対応作業の遂行に必要な範囲を超えて複製しない。

1-4（導入事例の紹介）

お客様へ導入した事例をお客様の了解を得ずに第三者に紹介しない。

1-5（関係者でなくなる場合）

当該お客様対応作業の関係者でなくなる場合（退職の場合は退職時点）、事前にお客様情報をお客様に返還する。ただし、お客様との書面により合意している場合、合意された方法に基づく廃棄でも可とする。

引継ぎ等で前任者としてお客様情報を参照する必要がある場合は、後任者の管理下で行う。

また、当該お客様対応作業の関係者でなくなった後も、関係者であった時に知り得たお客様情報を他言、漏えいしない。

1-6（不要になった複製物）

作成したお客様情報の複製物であって不要になったものは直ちに削除または廃棄する。ただし、お客様と特別の合意がある場合はその合意に従う。

２．個人情報の取扱い

本項目は本遵守事項にあるお客様情報のうち、個人情報の取扱いに関して特に実施する項目です。

2-1（目的外利用の禁止）

個人情報を取り扱う場合は、本人の了解が得られた利用目的の範囲内で取り扱う。

① 個人情報を本人から直接取得する場合は、利用目的等、関係する法令、ガイドライン等に定められた事項を本人に告知し、同意を得てから個人情報を取得し、取り扱う。

② 個人情報の取扱いを受託した場合は、関係する契約条件に従い、受託の目的の範囲内で取り扱う。

2-2（本人からの問い合わせ）

個人情報に関し問い合わせ（開示、訂正、追加もしくは削除、利用の停止、消去または第三者への提供の停止に関するものを含む）を受けた場合、お客様に相談する。なお、個人情報がお客様情報の場合は、お客様に対応を依頼する。

３．お客様情報の入手、預かり、廃棄等

3-1（提供されるお客様情報）

お客様情報（データ、書類等）は、不正に入手しない。また、お客様対応作業に必要の無いお客様情報は受け取らない。

お客様から提供されるお客様情報を受け取る際は以下を確認する。

① 守秘義務等を定めた契約または覚書の締結を要否

② 秘密情報の有無

③ 開示範囲の確認

3-2（無断持ち出しの禁止）

お客様の事前承諾なく、お客様情報をお客様システムから持ち出さない。

3-3（返還を伴うお客様情報の預かり）

お客様情報は原則としてお客様の管理下で保管いただくか、やむを得ずお客様情報の入ったデータ、書類を預かる場合、授受を担当する者はお客様の指示に従う。また、預かる際は以下を確認する。

① 秘密情報の有無を確認し、秘密情報が含まれている場合、会社の業務責任者を通じてお客様に秘密情報の特定（マル秘表示等）を依頼する。

② お客様と合意した返還（複製物を含む）の期日と方法を確認する。

3-4（入手した、または預かったお客様情報の管理）

入手した、または預かったお客様情報はお客様との取り決め（契約、覚書　等）に応じて適切に管理する。

3-5（テストデータの預かり）

テストに使用するデータは個人や会社等が特定できない内容で預かる事を原則とする。

① データを預かる際は、データの消去または書換え等により個人や会社等が特定できないことをあらかじめお客様に確認する。

② お客様の実データを使用せざるを得ない場合、特に情報漏えい防止対策を実施する。

③ データ管理においては、入手時、テスト実施時、保管時、返還時等、あらゆる場面におけるリスクを想定して、当該リスク対策を確実に実施する。

④ 原本と共に、そのすべての複製物についても厳重に管理する。

3-6（お客様情報の返還または廃棄）

返還期日が到来した場合、お客様から要求を受けた場合、または当該お客様対応作業が終了しもしくは当該お客様対応作業において不要となった場合、お客様情報（複製物を含む）をお客様と合意した方法により速やかに返還（複製物を含む）する。

3-7（電子機器の預かり）

お客様の電子機器を修理・調査・解析・システム開発等の目的で預かる場合、お客様の指示に従い、預り証を発行する。

3-8（記録装置の交換）

修理等でお客様の記録装置（メモリ、HDD 等）を取り外し交換する場合、データが消去済みか確認する。

＜記録装置交換時の注意＞

① 事前にお客様によるデータ消去済みかを確認する。未実施の場合、お客様に消去を依頼する。

② お客様がデータを消去できない場合は、そのデータについての取り扱いにつきお客様の指示に従う。

③ 電子機器の返還時に記録装置に余分な情報が付加されていないことを確認する。

3-9（保守作業：ハードウェア内の残留物）

お客様の端末設置場所での保守作業を行う場合、ハードウェア内の残留物（各種カード、現金、レシート類）の有無を確認し、適切な対応を実施する。

残留物がある場合、手を触れず、その処置についてお客様に確認し対応する。

3-10（電子機器の引取り廃棄）

法律に基づき、お客様の電子機器を引き取り廃棄する場合、データが消去済みか確認する。

＜引取り廃棄時の注意＞

① 事前にお客様によるデータ消去が実施済みか否かを確認し、未実施の場合、お客様に消去を依頼する。

② お客様からデータの消去も委託されている場合、お客様と事前に取り決めた処理（上書き消去、電気的/磁気的破壊、物理的破砕等）を実施する。

③ 電子機器及び格納されているデータは作業が完了するまで厳重に管理する。

４． 移動、運搬等における諸注意

4-1（飲酒）

お客様情報を持ち歩く場合は飲酒をしない。飲酒をする場合は持ち歩かない。

4-2（公共交通機関利用時）

乗り物内ではお客様情報の入ったバック等を管理の目が届きにくい場所に置かない。

① お客様情報の入ったバック等を網棚に置かない。

② 着席時、お客様情報の入ったバック等は必ずひざの上に置き手をかける。

③ お客様情報の入ったバックをやむを得ず床に置く場合、バックの手提げ部分やショルダーストラップから手を放さない。

④ 乗り物内でバック等を座席に置いて席を離れない（トイレ、デッキとの往復含む）

4-3（自動車利用時）

お客様情報の入ったバック等を自動車内（トランクを含む）に放置しない。

タクシー利用時には降車の際、お客様情報の入ったバック等の置忘れをしない。

4-4（駅、空港、ホテル、飲食店利用時等）

盗難の危険性が高い場所（駅、空港、ホテル、飲食店等）ではお客様情報の入ったバック等から目を離さない。

4-5（手提げ袋）

手提げ袋は、「材質が弱い」、「上部が開いている」、「普段持ち歩かないので忘れない」等の理由から、お客様情報の運搬には原則利用しない。

4-6（周囲からの盗み見）

公共の場所での書類確認やパソコン等操作は原則行わない。やむを得ず行う場合には周辺から盗み見されないように注意する。

4-7（不適切な発言、行動）

公共の場（飲食店、交通機関、トイレ、ロビー、エレベーター等）においてお客様に関する不適切な発言（誹謗、中傷、お客様情報の関する会話）や行動をしない。

4-8（寄り道等）

お客様情報の運搬中は寄り道や回り道をせず、目的地まで速やかに安全に運ぶ。

4-9（搬送方法）

やむを得ずお客様資産（お客様情報含む）の搬送が必要なった場合、その資産に応じた搬送方法を十分に検討し、了解を得た方法で送る。（一般の宅配便、郵便等は原則利用しない。）

4-10（肌身離さず所持）

お客様情報の入った PC 等の電子機器、記録媒体、書類は運搬に適したバック等に入れ、肌身離さず所持する。

4-11（最小限の情報を持ち歩き）

業務で持ち歩く電子機器、記録媒体に格納するお客様情報は必要最小限の情報に留める。

4-12（携帯電話・スマートフォン）

携帯電話・スマートフォンはセキュリティの設定を行い、ストラップ等で繋ぎ紛失や盗難に注意する。また、不要な情報（メール等）はこまめに消す。

５． メール、FAX 利用上の諸注意

5-1（個人アドレス、FAX への送信禁止）

個人所有のメールアドレス、FAX にお客様情報を送信、転送しない。

5-2（お客様情報の送信）

やむを得ずお客様情報を電子メールその他のオンラインデータ伝送により送信する場合、暗号化その他の方法により情報漏えい対策を講じる。

5-3（秘密情報を含むメール）

秘密情報が含まれているお客様情報をメールで送信する場合は、「秘密情報が含まれている」ことをメールの表題または本文に付記する。

5-4（メールの誤送信対策）

初回または重要情報をメールで送信するときは、誤送信を防ぐ工夫を行う。

＜誤送信対策例＞

送信先から事前に依頼メール（送信元や送信者が間違いないか確認できる情報）を受け取り、そのメールに対して返信する。

5-5（一斉同報）

メールマガジンや会員誌等、他にアドレスを知らせてはいけない宛先に一斉同報する場合（宛先がお取引先様の自社内の場合も含む）、同報先が公開されていないメーリングリスト、専用ツールを必ず使用する。BCC は、配送経路上のメールサーバのバージョンによっては、同報先が公開されることがあるので利用しない。

5-6（メールの削除、暗号化保存）

送受信したメールは、その内容を確認し、リスクの高い情報は速やかに消去または暗号化して保存する。

5-7（FAX の誤送信対策）

初回または重要情報を FAX で送信するときは、誤送信を防ぐ工夫を行う。

＜誤送信対策例＞

① 送信元から事前に電話し、テスト送信を行う。確認がとれた後にリダイアルで本送信する。

② 確認済みの短縮ダイアルを使用する。その際、短縮ダイアルの押し間違いに注意する。

5-8（FAX 番号の印刷）

申込み用紙等の印刷物に自部門等の FAX を記載するときは、その番号で確実に受信可能かを事前にテストする。

６． お客様情報の自社オフィス内での取り扱い

6-1（お客様情報の放置禁止）

お客様情報の入ったデータ、書類等を放置しない。

＜不適切な行動＞

① 机上への放置。

② 会議室・作業場所への放置（置忘れ）、ホワイトボードの消し忘れ。

③ プリンタ、FAX の印刷物や原稿の放置（取り忘れ）。

④ PC を画面表示したまま離席。

⑤ お客様情報が記載された紙の裏紙利用。

6-2（お客様情報のデータ情報管理）

お客様情報はアクセスコントロールが施された安全なサーバに保存する。

お客様対応作業に使用する PC には必要最小限の情報のみ格納する。

6-3（退社時の保管）

お客様情報の入った電子機器、記録媒体、書類は退社時に容易に持ち運びできないように保管する。特に秘密情報が含まれているお客様情報は、お客様または会社業務責任者の指示に従い、厳重に保管する。

① ノートＰＣ：施錠できるキャビネットや引き出しに保管、またはセキュリティワイヤー等を利用する。

② デクストップＰＣ：施錠できる事務所内に保管、またはセキュリティワイヤー等を利用する。

③ お客様情報を保管している場所の鍵も厳重に管理する。

6-4（不要となった電子機器、記録媒体、書類の廃棄）

お客様情報の入った電子機器、記録媒体、書類を廃棄する場合、情報が漏えいしない方法で処分する。

＜廃棄方法の例＞

① 専用データ消去ツールによりデータを消去する。

② ハードディスク、記録媒体を物理的に破壊する。

③ 書類をシュレッダによる裁断、溶解、または焼却する。

７． 自社オフィス外におけるＰＣ等の利用

7-1（自宅持ち帰りの禁止）

空き巣、強盗の被害に遭う恐れがあるため、お客様情報は自宅におかず、会社等安全な場所に保管する。

＜出張等でやむを得ず自宅に持ち帰る場合の盗難対策＞

ハードディスク全体を暗号化できるツールの入ったノートＰＣまたは暗号化機能がある USB メモリに格納し、データを暗号化する。

7-2（ＰＣ、ＵＳＢメモリ等の持ち出し）

ＰＣ、ＵＳＢメモリ等をオフィス外に持ち出す場合は、持ち出し規則に従い、必要な手続きを行う。

８． 情報漏えい対策（暗号化その他）

8-1（私品利用禁止）

お客様情報を格納する電子機器、記録媒体等は暗号化その他の情報漏えい対策を行う。

ホテル、インターネットカフェ等に設置されているＰＣも使用しない。

8-2（暗号化その他の情報漏えい対策）

お客様情報を格納する電子機器、記録媒体等は暗号化その他の情報漏えい対策を行う。

＜暗号化その他の情報漏えい対策＞

① ノートＰＣを利用する場合、ＰＣのハードディスク全体を暗号化できるツールを導入し、データを必ず暗号化する、またはシンクライアントシステムを利用する。

② 技術的に暗号化が困難な製品しか選択の余地がない場合、その製品に適した情報漏えい対策を講じる。

③ ＰＣ（デスクトップ型、ノート型を問わず）や記録媒体へのパスワードの設定も行う。

8-3（ノート、手帳）

ノート、手帳等にリスクの高い情報を記録する場合、記号、略称を用いて第三者が容易に判別できないように工夫する。

９． 情報漏えい対策（Ｐ２Ｐソフト等）

9-1（Ｐ２Ｐソフトのインストール禁止）

お客様対応作業で使用しているＰＣに、Winny、Share 等のＰ２Ｐファイル交換ソフト（以下「Ｐ２Ｐソフト」という）をインストールしない。

9-2（Ｐ２Ｐソフト搭載ＰＣの利用禁止）

Ｐ２ＰソフトがインストールされているＰＣ（以下「Ｐ２Ｐソフト搭載ＰＣ」という）を、いかなる形態（以下の内容も含む）でもお客様対応作業に使用しない。

① お客様対応作業に関する情報（お客様情報含む）の入った記録媒体の接続。

② お客様対応作業に関する情報（お客様情報含む）の入ったメールの送受信

③ Ｐ２Ｐソフト搭載ＰＣとお客様対応作業で使用しているＰＣをファイルやフォルダを共有する同一のＬＡＮ環境で使用。

④ お客様対応作業で使用しているネットワークへの接続（リモート接続を含む）

9-3（Ｐ２Ｐソフトに対する危険性の認識）

Ｐ２Ｐソフト搭載ＰＣについて以下の危険性を認識する。

① Ｐ２Ｐソフト搭載ＰＣに感染するウィルスには亜種が多く、ウィルス対策ソフトを使用し、パターンファイルを常に最新にしていても、情報が流出する。

② ウィルスによって流出したファイルは削除することが極めて困難である。

③ ウィルスによって業務情報のみならず同時に他人に知らせたくない個人的な情報（画像、メール履歴、その他個人情報等の入ったファイル）も流出する。

１０．ウィルス対策

10-1（ウィルス未確認ＰＣ等の持ち込み禁止）

ウィルス感染の疑いある、またはお客様対応作業に不必要なＰＣや記録媒体等は、お客様構内に持ち込まない。

10-2（同時接続禁止）

お客様のネットワークに接続したまま、別の通信回線（有線、無線を問わず）を利用して外部と接続しない。

10-3（お客様ネットワーク接続ＰＣのウィルスチェック）

お客様のネットワークに接続するＰＣやお客様に納入する記録媒体は、ウィルスチェックを実施する。

① 事前に最新のワクチンによるウィルスチェックを行い、ＰＣは再起動を行う。

② ＰＣには最新のセキュリティパッチを適用する。

10-4（預かりＰＣのウィルスチェック）

お客様からお預かりしたＰＣはお預かり時と返還時にウィルスチェックする。

10-5（外部接続ＰＣのウィルスチェック）

通信回線（有線、無線を問わず）を利用して外部と接続した場合、最新のワクチンによるウィルスチェックを行う。

10-6（ＰＣのウィルス対策）

お客様対応作業に利用するＰＣはウィルス対策ソフトを搭載し、パターンファイルは常に最新版に更新する。

10-7（電子メール受信時のウィルス注意）

電子メールを受信しても、添付ファイルを不用意に開けない。不審なメールは廃棄する。

＜不審なメールの例＞

① 身元が分からない者からのメール。

② メール本文の内容が不審である。

③ メール本文と関係が無いと思われる添付ファイルやＵＲＬが付いている。

１１．お客様の構内で行う作業

11-1（お客様設備等の私的・目的外利用の禁止）

お客様設備を私的目的で利用しない。

お客様イントラネットから事前にお客様と合意した使用目的以外で外部にアクセス（メールの送受信を含む）しない。

11-2（無断廃棄、持ち出し禁止）

作業で発生したデータ、書類等はお客様の承認なく無断廃棄、持ち出ししない。

11-3（作業の計画・結果）

お客様構内においてはお客様の承認に基づきお客様対応作業を行う。

① 作業計画、計画変更は事前にお客様の承認を得る。

② お客様の資産の借用や作業に必要な機器の持ち込みは事前にお客様の承認を得る。

③ 作業内容や結果を記録し、会社の業務責任者へ適宜報告する。（お客様から指定されている場合はお客様へも適宜報告する。）

④ 作業終了時は速やかに片付け、引き上げる。

11-4（お客様構内のルール）

お客様構内のルールを確認し、遵守する（区域、建物の注意表示板にも十分注意する。）

① お客様から許可／指示された区域以外へは立ち入らない。

② お客様構内ではお客様の許可無く撮影しない。コード読み取り（ＱＲコード等）携帯電話・スマートフォンのカメラ機能を使用する際もお客様の許可を得る。

③ ＰＣ、ＵＳＢメモリ、携帯電話等の持ち込みが禁止されている場合、そのルールに従う。

１２．入場証、操作者用カード、パスワード等の取扱い

12-1（入場証の管理）

お客様発行の入場許可証、マシン室入退出カード等（以下「入場証」という）は、厳重に管理する。

① 入場証を貸し借りしない。

② 入場証の紛失・盗難防止に細心の注意を払う。

③ 入場証取扱いに関するルール（常時着用、一人ひとりの入退記録を残す等）を遵守する。

④ 訪問者（ゲスト）として入退場する場合もお客様構内ルールを遵守する。

12-2（お客様システムの操作者用カード等の取扱い）

お客様システムを操作（開発、保守、運用等）する者が使用するカード（ＩＣカード、ＩＤカード等。以下「操作者用カード等」という）は、作業毎に事前に会社の業務責任者を通じてお客様に作業内容の承認を得たうえで借用し、借用中は厳重に管理

する。

＜操作者用カード等借用時の注意＞

① 操作者用カード等を貸し借りしない。

② 操作者用カード等の紛失・盗難防止に細心の注意を払う。

③ 操作者用カード等は予めお客様から指定された作業場所（マシン室等）から持ち出さない。

やむを得ず操作者用カード等を持ち出す場合、会社の業務責任者を通じて、事前に書面によるお客様の承認を得る。

＜操作者用カード等の返却＞

お客様システムを操作（開発、保守、運用等）する者は、会社の業務責任者に対し、借用期間中の操作者用カード等の保管をお客様または会社のいずれかが行うかにつき確認したうえで、以下を遵守する。

① 操作者用カード等の保管をお客様が行う場合、一日の作業終了後、直ちにお客様へ返却する。

② 操作者用カード等の保管を会社が行う場合、一日の作業終了後、直ちに施錠できる指定保管場所に確実に返却する。操作者用カード等の借用、返却はお客様が確認できる方法（台帳等）で記録する。

12-3（アカウント、パスワードの開示禁止）

アカウント、パスワードは自分以外の者へ開示しない。

12-4（アカウント、パスワードの問い合わせ対応）

アカウント、パスワードに関する問い合わせはお客様内部からであっても直接回答せず、お客様の管理部門責任者に対応を依頼する。

１３．お客様システム、ネットワークへの接続・修正等の作業

13-1（違法、不適切行為の禁止）

お客様システム、ネットワークへの接続・修正等の作業において、違法または不適切な行為を行わない。

＜違法または不適切な行為の例＞

① お客様が使用承諾を受けていないソフトウェア（フリーソフトを含む）のインストール。

② ＳＱＬインジェクション等第三者のシステムへの不正アクセス行為。

13-2（お客様の承認）

お客様システム、ネットワークへの接続・修正等の作業を行う場合、お客様の書面（電子メール等含む）による事前承認に基づき実施する。

＜お客様承認を必要とする作業例＞

① 本番環境へのアクセス

② システムに格納されているお客様情報へのアクセスや引き出し。

③ プログラム・パッチ修正

④ システムパラメータの変更やデータ修正（作業の前後にお客様、会社の業務責任者を含め、複数人で内容の確認を行う。）

⑤ 持ち込んだＰＣ等のお客様のネットワークへの接続。

⑥ その他、お客様の書面による事前承認を必要とする作業。

13-3（お客様システムのリスク確認）

お客様システムのセキュリティ状態（最新ワクチン適用の有無）をお客様に提示し、相互にリスクの有無を確認する。

13-4（開発環境へのアクセス）

お客様所有の開発環境へのアクセスもセキュリティに十分配慮する。

13-5（リモート接続）

お客様環境と会社の保有する機器をリモート接続し作業を行う際、以下の項目を遵守する。

① お客様了承のもと、作業を開始し、終了時にお客様へ報告を行う。独自判断で作業を開始しない。

② リモート接続日時、作業内容について台帳に記録し、会社の業務責任者の承認を得る。

③ 離席時は不正使用防止処置（スクリーンセーバー等）を施す。機器を使用しない時、電源をＯＦＦにする。

④　作業に必要のない機器、記録媒体等は接続しない。

１４．事故発生時の対応

14-1（事故発生）

事故発生時には以下の対応を行う。

①　一人で解決しようとせず、直ちに上司（会社の業務責任者を含む）に報告する。

②　会社の業務責任者を通じてお客様に第一報を行う。

③　紛失・盗難の場合は警察、交通機関にも届けを出す。